AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.(original) A method of detecting virus infection of an executable image comprising:

identifying by reference to a database of known executable image layouts, the layouts to which the executable image conforms;

identifying start-up code within the executable image by reference to the identified image layout; and

examining the start-up code with reference to a database of start-up code characteristics to determine whether the image is likely to have been subject to viral modification.

2.(original) A method according to claim 1, wherein the database of start-up code characteristics includes patterns characteristic of start-up code generated by a set of known compilers.

3.(original) A method according to claim 2 for scanning the executable image for patterns of start-up code expected to be present as a consequence of that compiler having been used to create the executable image and determining, in regard to patterns so found, whether there is evidence of viral code interposed in the execution path from the entry point of the executable image.

4.(original) A method according to claim 3 wherein, if it is determined that the executable image contains known start-up code but that execution of the image will not actually start with that code, flagging the image as suspicious from the point of view of possibly containing viral code.

5.(currently amended) A method according to claim 3 ~~or 4~~ wherein, if it is determined that the executable image starts with code similar to the known start-up code but the beginning of this code has been changed, flagging the image as suspicious from the point of view of possibly containing viral code.

6.(currently amended) A method according to ~~any one of the preceding claims~~claim 1, wherein the start up code database includes records of data values associated with routines which form part of the start up code and including the step of identifying the data in the executable image corresponding to at least one such data value and comparing it with that value.

7.(original) A system for detecting virus infection of an executable image comprising:

means for identifying, by reference to a database of known executable image layouts, to which one of those layouts the executable image conforms;

means for identifying start-up code within the executable image by reference to the identified image layout; and

means for examining the start-up code with reference to a database of start-up code characteristics to determine whether the image is likely to have been subject to viral modification.

8.(original) A system according to claim 7, wherein the database of start-up code characteristics includes patterns characteristic of start-up code generated by a set of known compilers.

9.(original) A system according to claim 8 for scanning the executable image for patterns of known startup code and determining, in regard to patterns so found, whether there is evidence of viral code interposed in the execution path from the entry point of the executable image.

10.(original) A system according to claim 9 wherein, if it is determined that the executable image contains known start-up code but that execution of the image will not actually start with that code, flagging the image as suspicious from the point of view of possibly containing viral code.

11.(currently amended) A system according to claim 9 ~~or 10~~ wherein, if it is determined that the executable image starts with code similar to the expected start-up code but the beginning of this code has been changed, flagging the image as suspicious from the point of view of possibly containing viral code.

12.(currently amended) A system according to ~~any one of claims 7-11~~claim 7 wherein, the start up code database includes records of data values associated with routines which form part of the start up code and including means for identifying the data in the executable image corresponding to at least one such data value and comparing it with that value.

13. (canceled)

14.(canceled)